E-VIDENCE: Requesting Electronic Evidence Across Borders for Investigating Online Criminal Matters, Including Terrorism

Terrorist use of the Internet

In today's interconnected world, the proliferation of cyber threats posed by organized crime groups and terrorists presents a significant challenge to global security in various areas. Leveraging the vast reach of the Internet, social media platforms, and encrypted messaging applications, terrorist actors exploit technology to advance their agendas and perpetrate crimes: Out of 223 convicted terrorists based in the UK, 54% learned some aspect about their intended activities online. This number has been steadily increasing to 76% between 2012 and 2017.

Why it matters

Effectively gathering electronic evidence (e-evidence) from digital platforms is essential to counteracting the proliferation of cyber threats posed by organized crime groups and terrorists on a broader scale. According to a 2023 survey conducted by the European Union, more than half of all criminal investigations involved a request for cross-border access to e-evidence. However, this endeavor is not without its obstacles. It requires overcoming technical barriers and navigating complex legal and jurisdictional issues, including discrepancies in national regulatory frameworks and the diverse terms of service of social media platforms or other Internet services.

A critical concern is the cross-border nature of e-evidence, often stored by service providers in jurisdictions different from where the crimes were committed. This geographical disparity can impede access to vital evidence and hinder the prosecution of perpetrators, undermining efforts to combat terrorism and organized crime. Furthermore, national legislation and local government planning can provide a framework for cross-border e-evidence requests. However, due to the lack of harmonization of the existing legal frameworks across different jurisdictions or the lack of an applicable treaty between the requesting and the requested country, significant legal barriers to accessing e-evidence can result in delays in investigations.

In this context, the significance of human rights cannot be overstated. In developing approaches to counter-terrorism, it is crucial to ensure that these approaches are deeply rooted in respecting human rights.

Addressing these challenges requires a comprehensive approach that emphasizes international cooperation, capacity building, and the promotion of fundamental human rights principles. Law enforcement agencies, prosecutors, and judges must possess the requisite knowledge and skills to effectively investigate cybercrimes while upholding fundamental human rights and legal and ethical standards.

Objective

Enhance national capacities across the OSCE region regarding the request of e-evidence for investigating and prosecuting online criminal matters, including terrorism related cases while adhering to the fundamental principles of human rights.

OSCE
Organization for Security and
Co-operation in Europe

Concrete Steps:

NEEDS ASSESSMENT AND FACILITATING HUMAN-RIGHTS BASED RESPONSES: Initiate national needs assessments that will include analyzing the current regulatory framework and legal environment to identify challenges and areas for improvement, including their compliance with respecting human rights. Based on the findings, strengthen the capacities of national stakeholders in up to ten OSCE participating states (pS) and Partners for Cooperation (PfC). When needed, providing support to updating regulatory frameworks through establishing the National Working Groups to promote the implementation of needs assessment recommendations.

CREATING STANDARD OPERATIONAL PROCEDURES AND DEVELOPING CAPACITIES: Enhance national regulatory frameworks and procedures to address limitations hindering law enforcement's ability to request and obtain electronic evidence from foreign service providers. Additionally, bolster operational capacities of respective pS and PfC in navigating cross-border electronic evidence requests while upholding human rights obligations. Facilitate the delivery of train-the-trainer courses on requesting electronic evidence across borders for the relevant national law enforcement and judicial institutions, using the available materials.

SUB-REGIONAL EVENTS: Organization of sub-regional events for relevant stakeholders representing Central Asia and South-Eastern Europe. The sub-regional events will seek to identify new and remaining challenges, opportunities, as well as lessons learned following the implementation of previous project activities.

DIALOGUE: Synchronize efforts on the substance across the OSCE region by identifying challenges, opportunities, and lessons learned by organizing a two-day OSCE-wide dialogue with participation of experts, relevant stakeholders from pS and PfC;

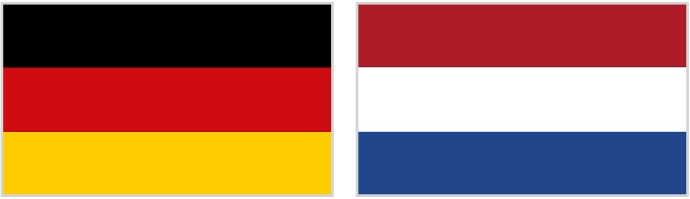
Expected Results

Result 1: Pinpointing the specific needs and priorities of OSCE pS and PfC regarding the cross-border acquisition of electronic evidence for combating online criminal activities, including terrorism-related cases with a human rights-centered approach.

Result 2: Fortifying regulatory frameworks and operational capabilities of pS and PfC in cross-border electronic evidence acquisition, particularly concerning terrorism-related cases by developing standard operational procedures (SOPs) and organizing advocacy events.

Result 3: Bolstering the technical capacities of national law enforcement agencies and judiciaries in cross-border electronic evidence acquisition, emphasizing adherence to human rights standards.

This extra-budgetary project is funded by:



OSCE
Organization for Security and
Co-operation in Europe